APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,278	01/11/2002	Christian Ensel	1454.1212	5517

21171 7590 04/08/2005	EXAMINER
STAAS & HALSEY LLP	LESNIEWSKI, VICTOR D
SUITE 700	

	ART UNIT	PAPER NUMBER
1201 NEW YORK AVENUE, N.W.		
WASHINGTON, DC 20005	2155	

DATE MAILED: 04/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/042,278	ENSEL ET AL.
	Examiner	Art Unit	
	Victor Lesniewski	2155	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _11 January 2002_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-29_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-29_ is/are rejected.

7)☒ Claim(s) _29_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All   b)☐ Some * c)☐ None of:

   1.☒ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _4/29/2004_.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This application has been examined.

2.   Claims 1-29 are pending.

Priority

3.   Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers

have been placed of record in the file.

Information Disclosure Statement

4.   The IDS filed 4/29/2004 has been considered.

Claim Objections

5.   Claim 29 is objected to because of the following informalities:

•   The 29th claim has been misnumbered as "28."

Appropriate correction is required.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7.   Claims 1-6, 8-20, and 22-29 are rejected under 35 U.S.C. 102(e) as being anticipated by

Campbell et al. (U.S. Patent Number 6,839,850), hereinafter referred to as Campbell.

8.   Some claims will be discussed together. Those claims which are essentially the same

except that they set forth the claimed invention as an alternative method, a device, or a computer-

readable storage medium are rejected under the same rationale applied to the described claim.

9.   Campbell has disclosed:

- <Claims 1, 27, and 28>

    A method for computer-aided monitoring of a telecommunication network formed of

    devices capable of communication, said method comprising: determining activity

    parameters, each describing activity of at least one of a corresponding device and a

    corresponding service (column 16, line 45 through column 18, line 40); comparing the

    activity parameters by a statistical estimator (figure 4, item 300) trained with training data

    and having a normal range of dependence based on dependences determined between the

    devices (column 18, lines 41-67); and determining from said comparing whether at least

    one of the devices and services in the telecommunication network has a communication

    performance different from the normal range of dependence in accordance with a

    predetermined criterion (column 14, lines 28-39).

- <Claims 2 and 16>

    The method as claimed in claim 1, wherein at least some of the devices are constructed as

    terminals capable of communication (column 8, lines 12-21).

- <Claims 3 and 17>

  The method as claimed in claim 1, wherein the activity parameters are determined within a predetermined time interval (column 17, lines 1-6).

- <Claims 4 and 18>

  The method as claimed in claim 1, wherein said determining of each activity parameter is performed by the corresponding device (column 10, lines 20-39 wherein the audit collection function is "on the monitored network node"), and wherein said method further comprises transmitting the activity parameters to an administration unit which performs said comparing and determining based on said comparing (figure 4, item 114).

- <Claims 5 and 19>

  The method as claimed in claim 1, wherein said determining of each activity parameter is performed by an activity parameter determining unit separate from the corresponding devices (column 10, lines 20-39 wherein the audit collection function is "logically near the monitored network node").

- <Claims 6 and 20>

  The method as claimed in claim 1, further comprising determining communication-dependent dependences between at least some of the devices and services (column 14, line 59 through column 15, line 4).

- <Claims 8 and 22>

  The method as claimed in claim 1, further comprising determining data of at least some of the devices and services (column 17, lines 45-47), and wherein said determining of the activity parameters is based on the data (column 17, lines 51-59).

- <Claims 9 and 23>

  The method as claimed in claim 1, wherein said determining of the activity parameters uses all possible pairs of the devices and pairs of services (column 13, lines 39-45).

- <Claims 10 and 24>

  The method as claimed in claim 9, further comprising: storing the activity parameters determined from the pairs of devices in a matrix (column 16, lines 56-63); and determining the normal range of dependence from a structure of the matrix (column 16, lines 63-67).

- <Claims 11 and 25>

  The method as claimed in claim 1, wherein at least one of the following parameters is determined as one of the activity parameters data packets sent or received by the at least one of a corresponding device and a corresponding service, processor utilization of the corresponding device, a number of predetermined system function calls, and existence of at least one of predetermined processes and predetermined computer programs (column 17, lines 1-6).

- <Claims 12 and 26>

  The method as claimed in claim 1, wherein a neuro-fuzzy model is used as the statistical estimator (column 16, lines 1-9).

- <Claim 13>

  The method as claimed in claim 1, further comprising generating an alarm signal when at least one device in the telecommunication network differs from the normal range of dependence in accordance with the predetermined criterion (column 13, lines 31-32).

- \<Claim 14\>

  The method as claimed in claim 1, further comprising at least one of determining a disturbance of one of the devices in the telecommunication network; determining an unauthorized attempt to access one of the devices; and determining an unauthorized access attempt by one of the devices (column 2, lines 25-38).

- \<Claims 15 and 28\>

  A method for computer-aided training of a statistical estimator for administering a telecommunication network formed of devices capable of communication, said method comprising: determining activity parameters, each describing activity of at least one of a corresponding device and a corresponding service (column 16, line 45 through column 18, line 40); determining possible dependences between the devices and services from the activity parameters (column 18, lines 41-67); and determining from the possible dependences a normal range of dependence for at least some of the devices and services in essentially undisturbed states to train the statistical estimator (column 6, lines 33-46).

Since all the limitations of the invention as set forth in claims 1-6, 8-20, and 22-29 were disclosed by Campbell, claims 1-6, 8-20, and 22-29 are rejected.

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11.   Claims 7 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Campbell.

12.   Campbell has disclosed a method for detecting intrusion into and misuse of a data

processing system. Although he did not explicitly disclose determining possible directional

dependences with regard to directions of communication between the devices, this would be a

clear extension of his system. Campbell's system can be utilized in a communications network

(see column 9, lines 35-46) and is set up to monitor and analyze different events or sessions in

the network (see column 14, line 59 through column 15, line 4). In such a communications

network it is clear that a particular event or an activity during a session could be either incoming

or outgoing data from or to another device. Thus, it would have been obvious to one of ordinary

skill in the art at the time of the applicant's invention to modify the system of Campbell by

adding the ability to determine possible directional dependences with regard to directions of

communication between the devices.

13.   Thereby, Campbell discloses:

• <Claims 7 and 21>

    The method as claimed in claim 1, further comprising determining possible directional

    dependences with regard to directions of communication between at least some of the

    devices and services (column 14, line 59 through column 15, line 4, and obviousness).

Since Campbell discloses all of the above limitations, claims 7 and 21 are rejected.

Conclusion

14.   The prior art made of record and not relied upon is considered pertinent to the applicant's

disclosure.

- Porras et al. (U.S. Patent Number 6,321,338) disclosed a method for network surveillance

   that includes receiving network packets and building long-term and short-term statistical

   profiles.

- Trcka et al. (U.S. Patent Number 6,453,345) disclosed a network surveillance system that

   passively monitors and records network traffic by continuously routing packets to a high-

   capacity data recorder for archival.

15.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Victor Lesniewski whose telephone number is 571-272-3987.

The examiner can normally be reached on Monday through Thursday.

   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Victor Lesniewski
Patent Examiner
Group Art Unit 2155

BHARAT BAROT
PRIMARY EXAMINER